

INFORMATION \Leftarrow SECURITY \Rightarrow

Lesson 1: Threats

Lesson 2: Protection

Lesson 3: Policies

Lesson 4: Security Audits

Lesson 5: Tools/Techniques

Lesson 6: Design/Planning

INFORMATION \Leftarrow SECURITY \Rightarrow

Security Project Management

Project Plan

Add RSA key Auth

Add Password Auth

Add SSL for Logins

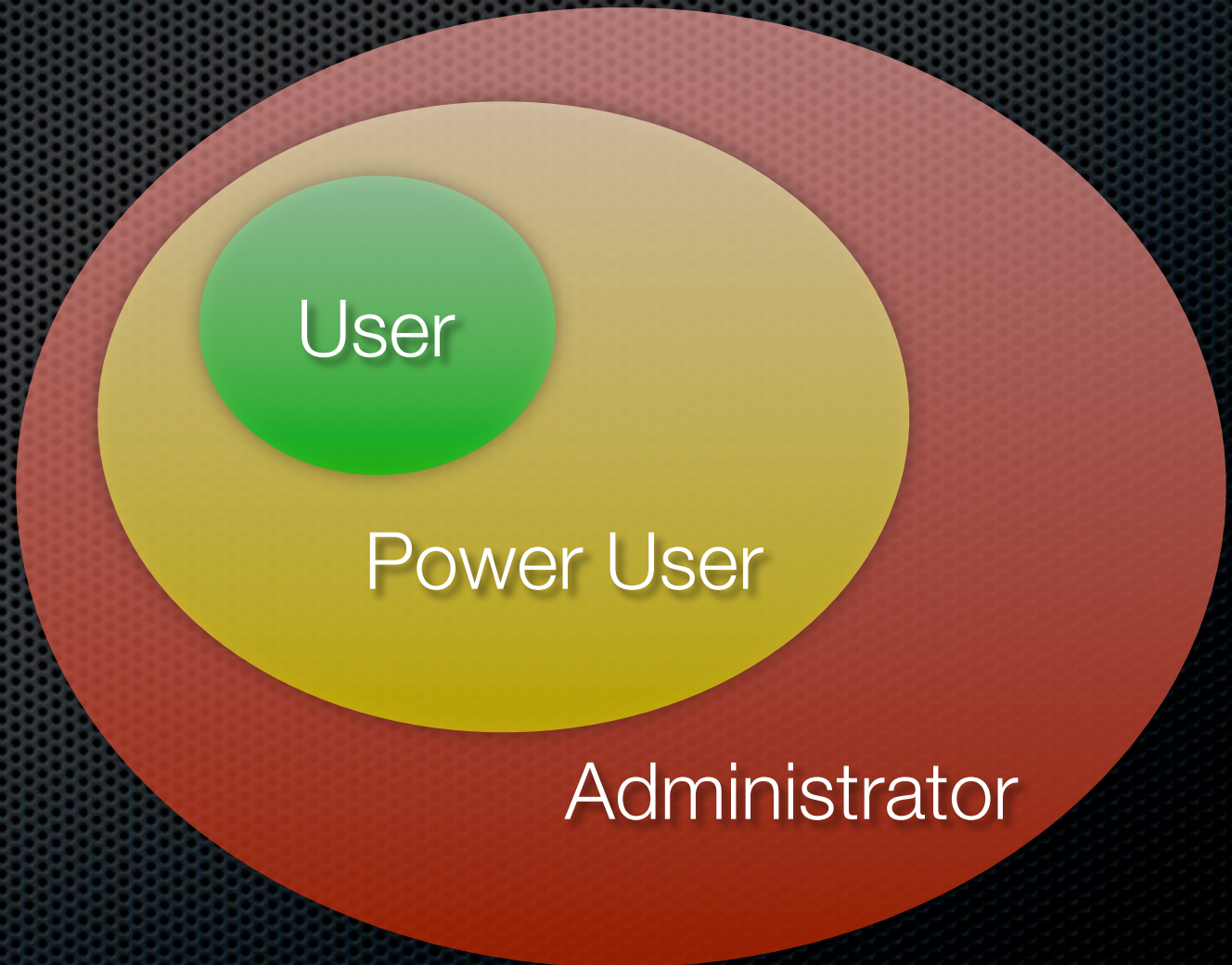
Setup User Accounts

- Build Security in to every project plan
- I wanted my company to standardize on SSL encryption every time a user sent us information via a website contact form.
- project management is supposed to be the art of planning ahead so you don't have to react later.

INFORMATION \Leftarrow SECURITY

Security Design

Least Privilege

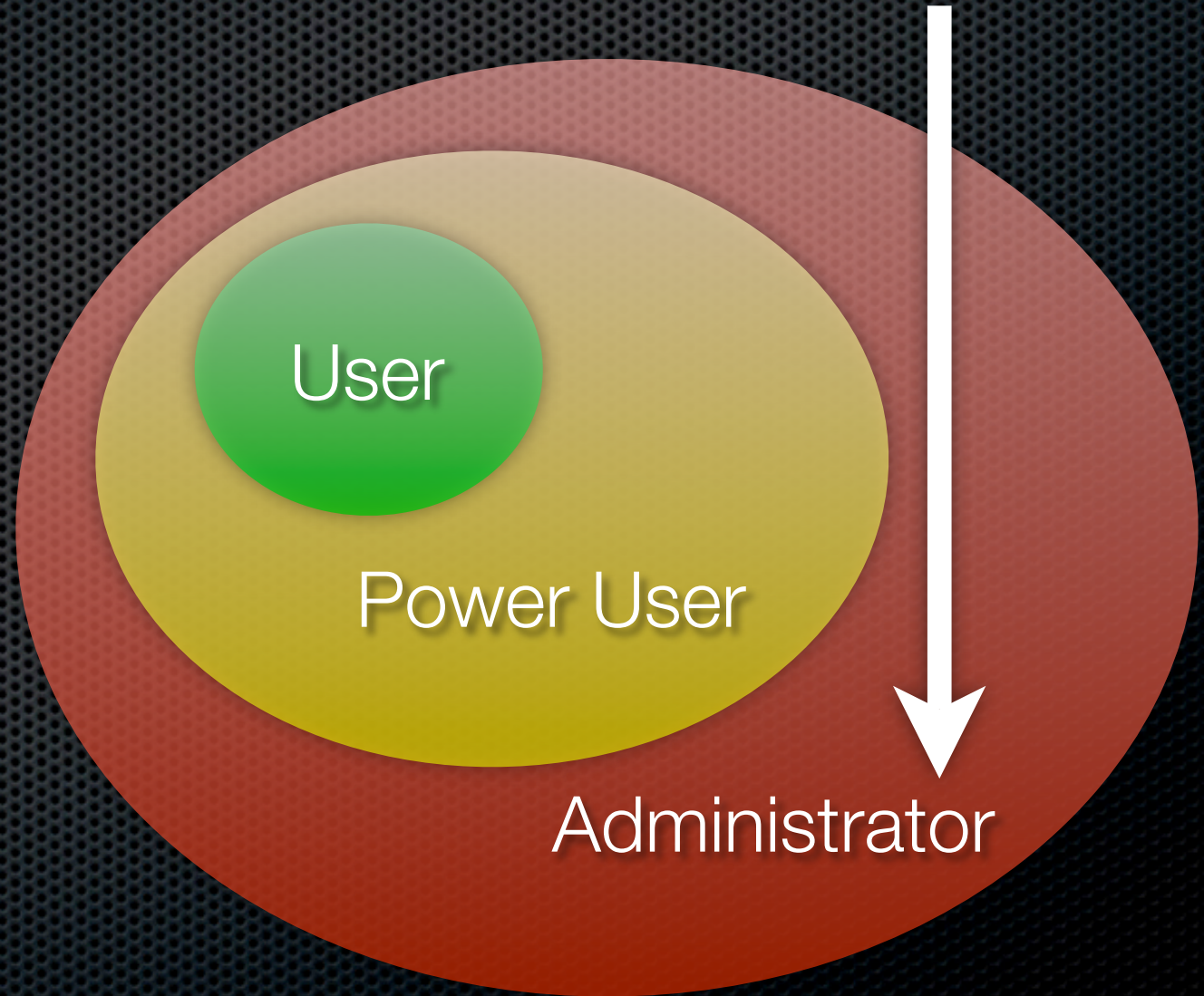


- You only have what you need
- AAA only has access to Switchboard.com and MapQuest.

INFORMATION \Leftarrow SECURITY

Security Design

Fail-Safe Defaults



- Default to NO ACCESS
- Think about Windows XP's default user account has Administrator access.

INFORMATION \Rightarrow SECURITY

Security Design

Economy of Mechanism

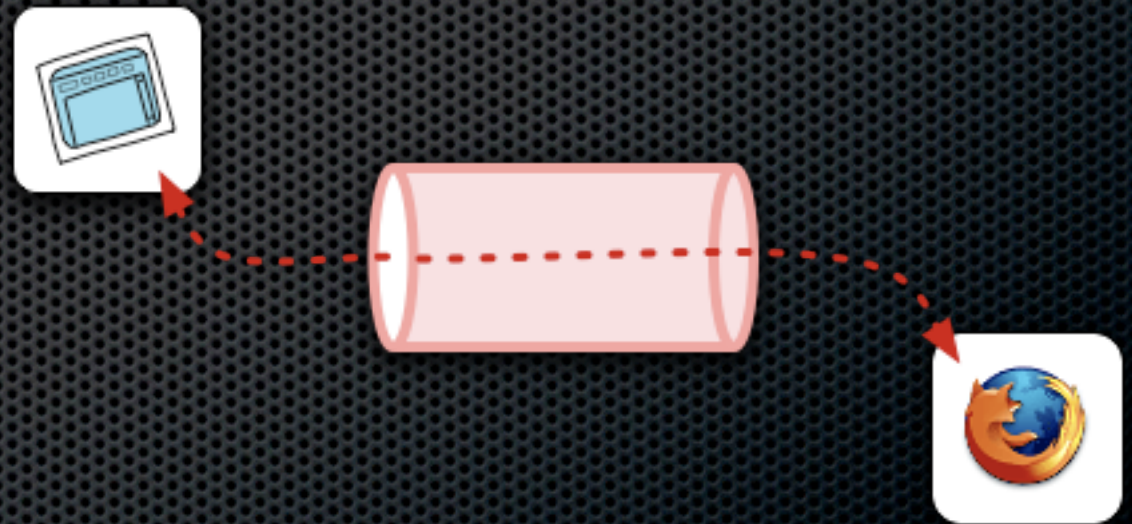
SIMPLE

- Keep it SIMPLE St00pid
- RSA keys are very simple. Users won't blurt out sensitive passwords, won't store those passwords on sticky notes. I have users posting passwords to public chat rooms. I can quickly disable an RSA key instead of having to change a whole system password and then redistribute that password.

INFORMATION \Rightarrow SECURITY

Security Design

Complete Mediation



- Transparent checking for virus' and spam
- Use VPN's, Use SSL, etc.
- Check ALL connections

INFORMATION

SECURITY

Security Design

Open Design

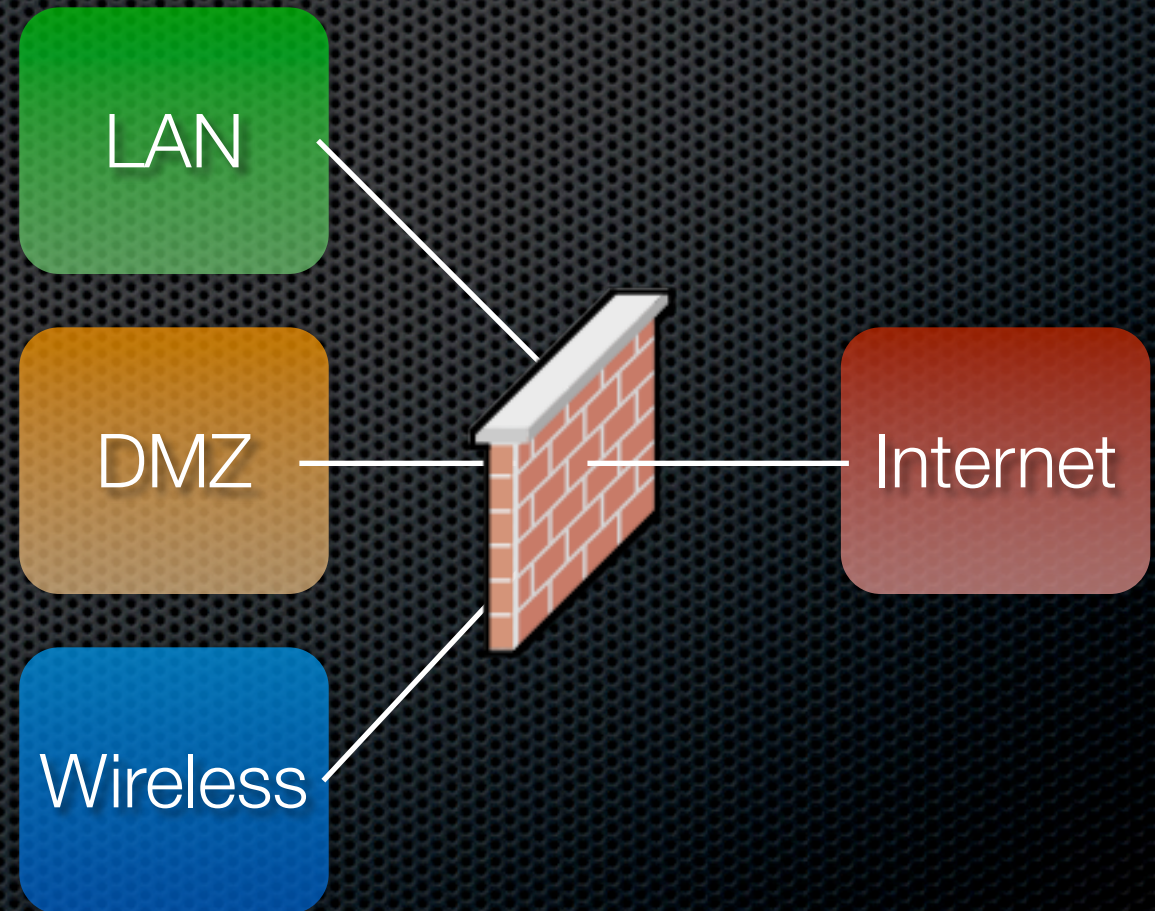


- Think Open Source
- Will your system/design stand up to peer review ?
- What improvements will somebody else think of ?

INFORMATION SECURITY

Security Design

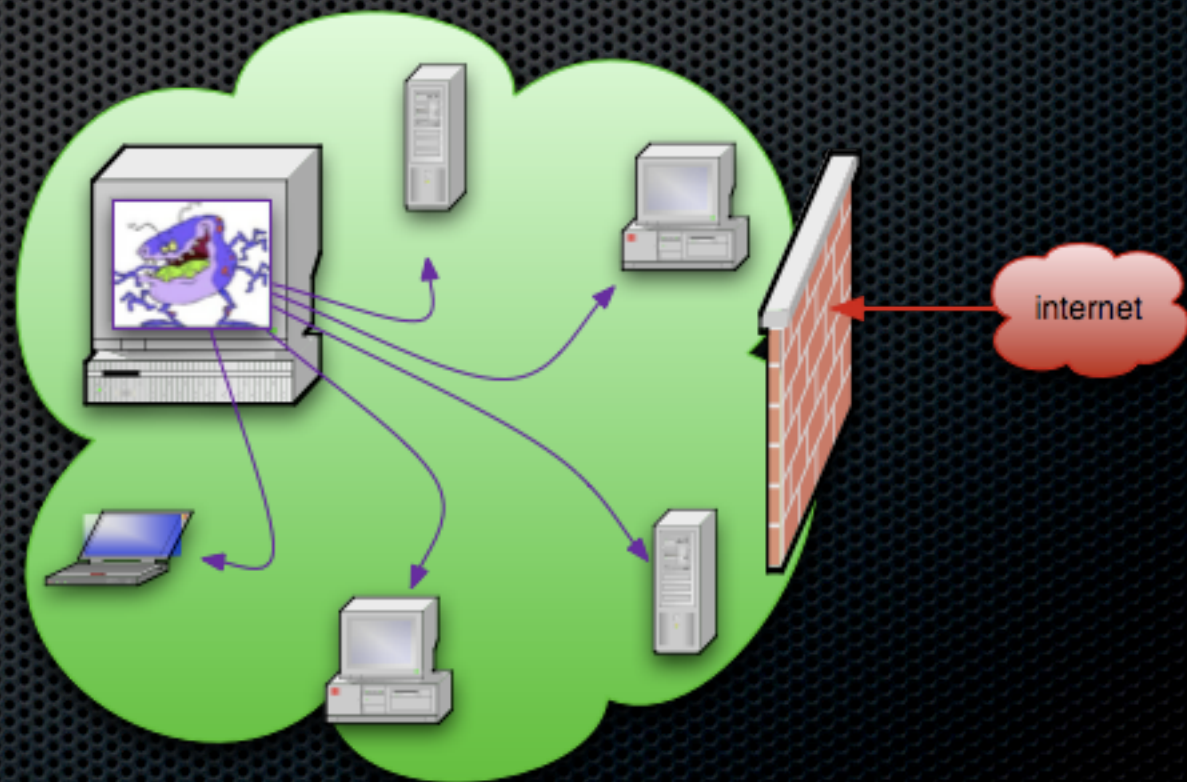
Separation of Privilege



- * LAN / DMZ network design
- * Internal and external communication
- * Administrator, Super User, Engineering, Common Users, etc.

INFORMATION SECURITY

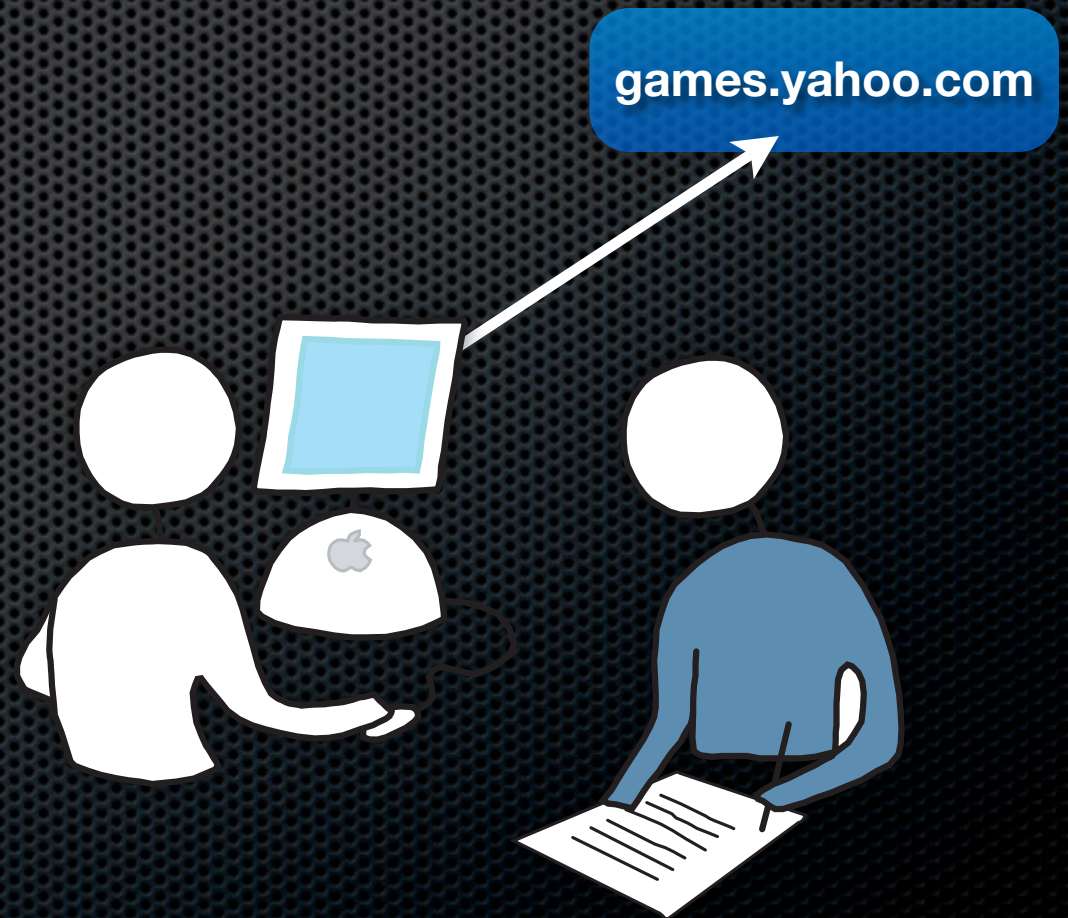
Security Design Least Common Mechanism



- You're only as good as your weakest link.
- Each computer needs a firewall, if a virus gets past the external firewall, then all the internal machines are boned.

INFORMATION SECURITY

Security Design
Psychological
Acceptability



games.yahoo.com

- One reason HTTPS (SSL) works is that people know to look for the little lock in their browser. If they don't see the lock, they don't enter their credit card, that simple.
- People need to accept the restrictions, or they will try to circumvent them. Think network firewalls or spam filters.